



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/692,884

10/20/2000

Kenneth R. Owens

4910.00003

6113

7590

09/07/2004

Joseph P. Krause
Vedder Price Kaufman & Kammholz
222 N. LaSalle Street
Chicago, IL 60601

EXAMINER

MATTIS, JASON E

ART UNIT

PAPER NUMBER

2665

DATE MAILED: 09/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/692,884

Applicant(s)

OWENS ET AL.

Examiner

Jason E Mattis

Art Unit

2665

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 July 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. This Action is in response to the after final amendment received on 7/22/2004. Claims 1-16 are currently pending in the application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 2, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cao et al. (U.S. Application 09/318694) in view of McAllister et al. (U.S. Pat. 6697329).

With respect to claim 1, Cao et al. discloses a multi-protocol label switching system comprised of a plurality of data switches, label switching routers, that are interconnected by a plurality of data paths from a source node, LSR S, to a destination node, LSR E, through a first set of data switches, LSR A and LSR B (**See paragraph 22 and Figure 1 of Cao et al. for reference to an MPLS data network comprised of label switching routers interconnected by paths**). Cao et al. also discloses a method within the MPLS data network of establishing a data flow over a protection path from a source switch, LSR S, to a destination switch, LSR E, through a second set of

switches, LSR C and LSR D (**See paragraph 24 and Figure 1 of Cao et al. for reference to switching to a secondary path when a primary path fails**). Cao et al. further discloses sending a first message to establish a working data path and a protection path from a first switch, LSR S, to a second switch, LSR E (**See paragraph 23-24 and Figure 1 of Cao et al. for reference to sending a router request downstream to request an explicitly routed path between source LSR S and destination LSR E and for reference to establishing a secondary route between source LSR S and destination LSR E**). Cao et al. does not disclose sending a second message from the second switch to the first switch establishing a reverse notification path through the network between the second and first switches. Cao et al. also does not disclose sending a third message over the reverse notification path to control protection switching by the first switch.

McAllister et al., in the field of communications, discloses sending a message establishing a reverse notification path through the network between the first and second switches (**See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to using a path from a second node to a first node to send acknowledgement messages from the second node to the first node in response to protocol messages, the second message, sent from the first node**). McAllister et al. also discloses sending a third message over the reverse notification path to control protection switching by the first switch (**See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to sending a an acknowledgement, a third message, which the first node uses to control protection switching, from the**

second node to the first node). Setting up a reverse notification path and sending signals over the path to a first, source, node has the advantage of allowing a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be “lost” on the failed path before the source node switches to the secondary path and also allowing the source node to resend packets on the secondary path that may have been “lost” while the destination node was receiving packets through the failed path.

It would have been obvious to one of ordinary skill in the art at the time of the invention, when presented with the work of McAllister et al., to combine setting up a reverse notification path and sending signals over the path to a first node to allow the first node to control protection switching, as suggested by McAllister et al., with the MPLS protection path system of Cao et al. with the motivation being to allow a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be “lost” on the failed path before the source node switches to the secondary path and also allow the source node to resend packets on the secondary path that may have been “lost” while the destination node was receiving packets through the failed path.

With respect to claim 2, Cao et al. discloses that the step of sending a first message is comprised of the step of adding a protection messaging field, which carries protection pathway information between switching elements, to a label distribution protocol message **(See column 24 and Figure 1 of Cao et al. for reference to using**

label distribution protocol to establish label switching paths to set up primary and protection data paths).

With respect to claim 4, Cao et al. discloses that the step of sending a message to establish a working path and a protection path between the first and second switches, LSR S and LSR E, includes the step of identifying at least one data switch, LSR S, as a switch element by the contents of at least one control field sent to at least one data switch, LSR E, of the MPLS network **(See paragraph 23-24 and Figure 1 of Cao et al. for reference to LSR S using control fields sent through the network to LSR E to request an explicitly routed path identifying itself as the source LSR).**

With respect to claim 5, Cao et al. discloses that the step of sending a first predetermined message to establish a working path and a protection path between the first and second switches, LSR S and LSR E, includes the step of identifying at least one data switch as a protection switch element, LSR C and LSR D, by the contents of at least one control field sent to at least one data, switch LSR E, of the MPLS network **(See paragraphs 23-24 and Figure 1 of Cao et al. for reference to LSR S using control fields to identify LSR C and LSR D as protection switch elements and sending this control information through the network to LSR E).**

With respect to claim 7, Cao et al. discloses the working path being set up loosely **(See paragraph 2 of Cao et al. for reference to prior art using loosely connected working and protection paths set up hop-by-hop).**

With respect to claim 8, Cao et al. discloses the working path being set up explicitly **(See paragraph 21 of Cao et al. for reference to explicitly setting up working and protection routing paths)**.

With respect to claim 9, Cao et al. discloses a step for mapping labels to data routed along the working path according to predetermined criteria that includes the quality of service granted to the data **(See paragraph 53 and Figure 2 of Cao et al. for reference to mapping labels routed along the first path according to predetermined criteria including a type of service field, which includes quality of service information)**.

With respect to claim 10, Cao et al. discloses a multi-protocol label switching system comprised of a plurality of data switches, label switching routers, that are interconnected by a plurality of data paths from a source node, LSR S, to a destination node, LSR E, through the data switches, LSR A and LSR B **(See paragraph 22 and Figure 1 of Cao et al. for reference to an MPLS data network comprised of label switching routers interconnected by paths)**. Cao et al. also discloses a method within the MPLS data network of routing data from a working path through the network to a protection path through the network **(See paragraph 24 and Figure 1 of Cao et al. for reference to switching to a secondary path when a primary path fails)**. Cao et al. further discloses sending a first control message to establish a working data path and a separate protection path from a first switch, LSR S, to a second switch, LSR E **(See paragraph 23-24 and Figure 1 of Cao et al. for reference to sending a router request downstream to request an explicitly routed path between source LSR S**

and destination LSR E and for reference to establishing a secondary route between source LSR S and destination LSR E). Cao et al. does not disclose sending a second message from the second switch to the first switch establishing a reverse notification path through the network between the second and first switches. Cao et al. also does not disclose sending a third message over the reverse notification path from the second switching to the first switch, the interruption of which controls protection switching by the first switch.

McAllister et al., in the field of communications, discloses sending a message establishing a reverse notification path through the network between the first and second switches **(See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to using a path from a second node to a first node to send acknowledgement messages from the second node to the first node in response to protocol messages, the second message, sent from the first node).** McAllister et al. also discloses sending a third message over the reverse notification path the interruption of which controls protection switching by the first switch **(See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to send a an acknowledgement, a third message, which the first node uses, by determining when the acknowledgement message was not received, or interrupted, to control protection switching from the second node to the first node).** Setting up a reverse notification path and sending signals over the path to a first, source, node has the advantage of allowing a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be "lost" on the failed path before the source

node switches to the secondary path and also allowing the source node to resend packets on the secondary path that may have been “lost” while the destination node was receiving packets through the failed path.

It would have been obvious to one of ordinary skill in the art at the time of the invention, when presented with the work of McAllister et al., to combine setting up a reverse notification path and sending signals over the path to a first node to allow the first node to control protection switching, as suggested by McAllister et al., with the MPLS protection path system of Cao et al. with the motivation being to allow a first, source, node to learn about a failure in a data path and immediately stop sending packets that will be “lost” on the failed path before the source node switches to the secondary path and also allow the source node to resend packets on the secondary path that may have been “lost” while the destination node was receiving packets through the failed path.

With respect to claim 11, Cao et al. discloses that sending a first message is comprises adding a protection messaging field, which carries protection pathway information between switching elements, to a label distribution protocol message (**See column 24 and Figure 1 of Cao et al. for reference to using label distribution protocol to establish label switching paths to set up primary and protection data paths**).

With respect to claim 13, Cao et al. discloses that sending a first predetermined control message from a first switch to a second switch comprises includes identifying at least one switch as a protection switch element, LSR C and LSR D, by the contents of

at least one control field sent to at least one switch, LSR E (**See paragraphs 23-24 and Figure 1 of Cao et al. for reference to LSR S using control fields to identify LSR C and LSR D as protection switch elements and sending this control information through the network to LSR E).**

With respect to claim 14, Cao et al. discloses the working path being set up loosely (**See paragraph 2 of Cao et al. for reference to prior art using loosely connected working and protection paths set up hop-by-hop).**

With respect to claim 15, Cao et al. discloses the working path being set up explicitly (**See paragraph 21 of Cao et al. for reference to explicitly setting up working and protection routing paths).**

With respect to claim 16, Cao et al. discloses mapping labels to data routed along the working path according to predetermined criteria that includes the quality of service granted to routed data (**See paragraph 53 and Figure 2 of Cao et al. for reference to mapping labels routed along the first path according to predetermined criteria including a type of service field, which includes quality of service information).**

4. Claims 3 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coe et al. in view of McAllister et al. as applied to claims 1, 2, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, and 16 above, and further in view of Aukia et al. (U.S. Pat. 6594268).

With respect to claims 3 and 12, the combination of Cao et al. and McAllister et al. does not disclose that sending a first message is comprised of the step of adding a

protection messaging field, which carries protection pathway information between switching elements, to an MPLS reservation protocol message.

Aukia et al., in the field of communications, discloses that sending a message is comprised of the step of adding a protection messaging field, which carries protection pathway information between switching elements, to an MPLS reservation protocol message (**See column 9 line 60 to column 10 line 47 and Figure 2 of Aukia et al. for reference to control messages using RSVP protocol, which are used to carry protection pathway information between network nodes**). Using an MPLS reservation protocol message to carry protection pathway information between switching elements has the advantage of being able to share protection pathway information between network elements using the current MPLS protocol, meaning that the current MPLS protocol would not have to be changed in order to implement the invention.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Aukia et al. to combine the use of an MPLS reservation protocol message of Aukia et al. with the MPLS protection path method of Cao et al. and McAllister et al., with the motivation being to be able to share protection pathway information between network elements using the current MPLS protocol, meaning that the current MPLS protocol would not have to be changed in order to implement the invention.

5. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cao et al. in view of McAllister et al. as applied to claims 1, 2, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, and 16 above, and further in view of Lemieux (U.S. Pat. 6452942).

With respect to claim 6, the combination of Cao et al. and McAllister et al does not specifically disclose a step of label binding the first message for the second switch to a third switch.

Lemieux, in the field of communications, discloses using label binding to distribute information to other label switches in a network (**See column 5 line 45 to column 6 line 4 of Lemieux for reference to using label binding to distribute information to other label switches in a network**). Using label binding has the advantage of being able to explicitly map data to specific label switching paths.

It would have been obvious to one of ordinary skill in the art at the time of the invention, when presented with the work of Lemieux, to combine the label binding of Lemieux with the MPLS data network protection paths of Cao et al. and McAllister et al., with the motivation being to be able to explicitly map data to specific label switching paths.

Response to Arguments

6. Applicant's arguments filed on 7/22/2004 have been fully considered but they are not persuasive.

In response to Applicant's argument that:

“the Examiner wholly ignored that Cao teaches it is preferable to have the sink router decide when to perform a protection switchover and which secondary stream to use.”

Examiner respectfully disagrees. Although the routers disclosed by Cao et al. do use the sink routers to determine when to perform a switchover and which secondary path to use, there is no indication in the Cao et al. reference that using a sink router to perform these functions is preferable to using a source router to perform these functions.

In response to Applicant's argument that:

“As set forth above McAllister is replete with teachings that a human preferably sets up paths through a network yet Cao teach that routers should set up paths through a network, Combining two references that teach contradictory methods doesn't make sense.”

Examiner respectfully disagrees. Although the paths of McAllister et al. are set up manually and the paths of Cao et al. are set up by the routers, these do not preclude the combination of the two references. The rejections above are not based on a combination of the routing network of Cao et al. with the routing network of McAllister et al. The McAllister et al. reference is merely used as a teaching of sending a message over an established reverse notification path to control protection switch. For reverse notification signaling to be used, it does not matter how the routing paths have been set up.

In response to Applicant's argument that:

“As set forth above, Cao teaches advantages to having the sink router select a protection path and when to perform a switchover, i.e. instantaneous switchover without data loss. McAllister on the other hand teaches that upon the detection of a failure node or link, some sort of message is sent upstream with a switchover being accomplished somehow by the source router ... The two different methodologies of Cao and McAllister cannot be reconciled in any way that would suggest they be combined.”

Examiner respectfully disagrees. First, although Cao et al. does teach using the sink router to select a protection path and when to perform switchover, the advantage of an instantaneous switchover is due to the fact that the secondary path has already been established, not due to the sink router deciding when to perform the switchover. The factor limiting the failure recovery speed of the Cao et al. routers is the speed at which failure information is propagated to the node performing the switchover. Further Cao et al. discloses that the failure information is propagated to both the source and the sink routers of the failed path (See page 2 paragraph 11 of Cao et al.). Therefore, having the source router perform the function of selecting a protection path and switching to the protection path, as suggested by McAllister et al., does not eliminate the advantage of an instantaneous switchover without data loss of the system and method of Cao et al.

In response to Applicant's argument that:

“In other words, the source node of McAllister does not attempt to re-route data along a different path until after the source receives a failure signal.

McAllister, therefore, does not predetermine a protection path as claimed by the Applicant in independent claims 1 and 10.”

Examiner agrees that the cited areas of McAllister et al. do not teach setting up a predetermined protection path; however, the claim limitation of setting up a predetermined protection path is found in the cited areas of the Cao et al. reference as shown in the rejections above. Again, the McAllister et al. reference is merely used as a teaching of sending a message over an established reverse notification path to control protection switch, not as a teaching of setting up a predetermined protection path.

In response to Applicant’s argument that;

“Neither of the two (2) reference show or suggest a predetermined control message that is sent from the egress router to the source router that establishes a reverse notification path.”

Examiner respectfully disagrees. As cited in the rejections above, McAllister et al. discloses periodically sending a control message and an acknowledgment message from source nodes to egress nodes and from egress nodes to source nodes establishing a reverse notification path associated with the nodes along a path or virtual connection (See column 9 line 47 to column 10 line 8 of McAllister et al. for reference to sending a an acknowledgement, a third message, which the first node uses to control protection switching, from the second node to the first node). Further, although Cao et al. does not specifically disclose setting up a reverse notification path, Cao et al. does disclose sending failure information upstream to the source router (See page 2

paragraph 11 of Cao et al.).

The rejections in this Action are based on the amended claims filed in the amendment received on 3/15/2004.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

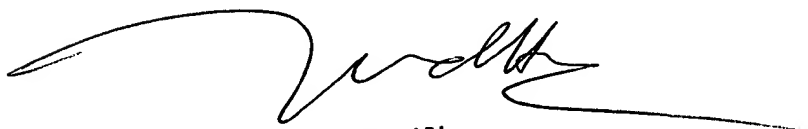
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason E Mattis whose telephone number is (571) 272-3154. The examiner can normally be reached on M-F 8AM-4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on (571) 272-3155. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jem



HUY D. VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600